Discrete Applied Mathematics 18 (1987) 25-38
North-Holland

ON THE COMPLEXITY OF CUTTING-PLANE PROOFS

W. COOK *
School of Operations Research and Industrial Engineering, Cornell University, USA

C.R. COULLARD
Department of Industrial Engineering, Purdue University, USA

Gy. TURÁN **
Automata Theory Research Group, Hungarian Academy of Sciences, József Attila University, Szeged, Hungary.

Received 24 June 1986
Revised 22 December 1986

As introduced by Chvátal, cutting planes provide a canonical way of proving that every integral solution of a given system of linear inequalities satisfies another specified inequality. In this note we make several observations on the complexity of such proofs in general and when restricted to proving the unsatisfiability of formulae in the propositional calculus.

1. Introduction

An attractive way of looking at Gomory's cutting plane technique [13] was introduced by Chvátal [5]. The point of view is that cutting planes provide a canonical way of proving that every integral solution of a given system of linear inequalities satisfies another given inequality. Suppose that we have such a system

$$a_i x \leq b_i \quad (i = 1, \ldots, m) \tag{1}$$

where $a_1, \ldots, a_m$ are rational vectors and $b_1, \ldots, b_m$ are rational numbers. If we also have nonnegative numbers y_i, $i = 1, \ldots, m$ such that $\sum \{y_i a_i : i = 1, \ldots, m\}$ is integral, then every integral solution of (1) satisfies the inequality

$$(\sum \{y_i a_i : i = 1, \ldots, m\})x \leq \gamma \tag{2}$$

for any γ which is at least $\lfloor \sum \{y_i b_i : i = 1, \ldots, m\} \rfloor$ (where $\lfloor q \rfloor$ denotes the largest

*Supported by a grant from the Alexander von Humboldt Stiftung and by the Institut für Ökonometrie und Operations Research of the University of Bonn, W. Germany.

**Supported by the joint research project "Algorithmic Aspects of Combinatorial Optimization" of the Hungarian Academy of Sciences (Magyar Tudományos Akadémia) and the German Research Association (Deutsche Forschungsgemeinschaft) and SFB 303 (DFG).

integer less than or equal to a given number q). We say that the inequality (2) is *derived* from (1). As in Chvátal [7], a *cutting-plane proof* of an inequality $cx \leq \alpha$ from (1) is a sequence of inequalities

$$a_{m+k}x \leq b_{m+k} \quad (k = 1, \ldots, M) \tag{3}$$

together with nonnegative numbers y_{kj} $(1 \leq k \leq M,\ 1 \leq j \leq m+k-1)$ such that for each $k = 1, \ldots, M$ the inequality $a_{m+k}x \leq b_{m+k}$ is derived from the system

$$a_i x \leq b_i \quad (i = 1, \ldots, m+k-1) \tag{4}$$

using the numbers $y_{kj}, j = 1, \ldots, m+k-1$, and such that the last inequality in the sequence is a positive scalar multiple of $cx \leq \alpha$.

So if there exists a cutting-plane proof of $cx \leq \alpha$ from (1), then every integral solution of (1) also satisfies $cx \leq \alpha$. Chvátal [5] showed that if the polyhedron defined by (1) is nonempty and bounded, then the converse of this statement is also true, that is if every integral solution of (1) satisfies $cx \leq \alpha$ then there exists a cutting-plane proof of $cx \leq \alpha$ from (1). Schrijver [27] latter showed, by a geometric argument, that the condition that the polyhedron be bounded can be removed as long as there exists at least one integral solution to (1). Examples of the use of cutting-plane proofs in the solution of combinatorial problems are given in Chvátal [5, 6, 7, 8] and Boyd and Pulleyblank [3].

The number M in (3) is the *length* of the cutting-plane proof of $cx \leq \alpha$ from (1). The applicability of cutting-plane proofs is clearly related to their length, which was investigated by Chvátal [7] for proofs of the stability number of graphs. In this note we make several observations on the length of cutting-plane proofs in general and when restricted to proving the unsatisfiability of formulae in the propositional calculus.

In Section 2 we show that if (1) has no integral solution then there exists a cutting-plane proof of $0x \leq -1$ from (1) whose length depends only on the number of variables in the system. Thus, there is an 'indirect' form of cutting-plane proof whose length can be bounded above by a constant in fixed dimension, contrasting the fact that an example of Bondy shows that even when restricted to problems in two dimensions the length of a shortest cutting-plane proof of $cx \leq \alpha$ from (1) cannot be bounded above by a polynomial function in the size (in binary notation) of (1) and $cx \leq \alpha$. We also discuss the size of coefficients appearing in cutting-plane proofs.

It is an important open problem in complexity theory to determine whether there exists a polynomial proof system for demonstrating the unsatisfiability of propositional formulae in conjunctive normal form; the existence of such a proof system is equivalent to NP = co-NP. Recently, Haken [16] settled a longstanding open problem by proving that the resolution proof system is not polynomial. No such result is known, however, for the extended version of resolution introduced by Tseitin [30]. Using Haken's result and a result of Cook [9], we show in Section 3 that cutting planes are between these two systems in power, that is, a polynomial-

length resolution proof implies a polynomial-length cutting-plane proof and the converse is not true, while a polynomial-length cutting-plane proof implies a polynomial-length extended resolution proof. Thus, an interesting next step in proving the nonpolynomiality of proof systems would be proving that the cutting-plane proof system is nonpolynomial. (We note that the hard formulae of Tseitin [30] are candidates for showing this.)

Throughout the paper we assume that all linear systems and polyhedra are rational. We refer the reader to the book of Schrijver [28] for the theory of polyhedra. The set of n component rational vectors and the set of n component integral vectors are denoted by $\mathbb{Q}^n$ and $\mathbb{Z}^n$ respectively. By the *size* of a linear system we mean the size of the system in binary notation (see, for example Lovász [24]).

2. Indirect cutting-plane proofs

In [7], Chvátal proved an upper bound on the length of cutting-plane proofs for the stability number of a graph in terms of the number of nodes, that is, in terms of the number of variables in the inequality. No such result holds in general, as is shown by the following example of J.A. Bondy (see Chvátal [5] and Schrijver [27]). Consider the linear system

$$\begin{aligned} -2tx_1 + x_2 &\leq 0, \\ 2tx_1 + x_2 &\leq 2t, \\ -x_2 &\leq 0 \end{aligned} \tag{5}$$

where t is a positive integer. It can be checked, by induction on t, that every cutting-plane proof of $x_2 \leq 0$ from (5) has length at least t. (Notice that t is not polynomially bounded in the size of (5) and $x_2 \leq 0$.) This is somewhat disappointing since we know that in fixed dimension we can prove the validity of $cx \leq \alpha$ for all integral solutions to $Ax \leq b$ in polynomial-time with Lenstra's algorithm [22]. To overcome this we will modify slightly the definition of a cutting-plane proof.

Observe that the inequality $cx \leq \alpha$, where c and α are integral, is satisfied by every integral solution of (1) if and only if the system

$$\begin{aligned} &a_i x \leq b_i \quad (i = 1, \ldots, m), \\ &cx \geq \alpha + 1 \end{aligned} \tag{6}$$

has no integral solution. This later property can be verified by exhibiting cutting-plane proof of $0x \leq -1$ from (6). We shall refer to such a verification of $cx \leq \alpha$ as an *indirect cutting-plane* proof of $cx \leq \alpha$ from (1) and define its length to be the length of the cutting-plane proof of $0x \leq -1$ from (6). (In general, if c and α are nonintegral, we first multiply the inequality by a positive number to obtain integral data.) With these definitions we have the following result.

Theorem 1. *For each natural number n there exists an integer f_n such that if every integral solution of a linear system $Ax \leq b$ in n variables satisfies an inequality $cx \leq \alpha$, then there exists an indirect cutting-plane proof of $cx \leq \alpha$ from $Ax \leq b$ whose length is at most f_n.*

To prove this result, we first state it in a different way. As in Schrijver [27], cutting-plane proofs may be viewed geometrically as follows. Let P be a polyhedron and $H = \{x : cx \leq \alpha\}$ a halfspace which contains P, where c is an integral vector with relatively prime components. It is clear that every integral point in P is contained in the halfspace $H_1 = \{x : cx \leq \lfloor \alpha \rfloor\}$. (Note that H_1 is obtained by shifting the supporting hyperplane of H until it contains integral points.) We refer to such a halfspace H_1 as a *Chvátal cut* for P and say that $P \cap H_1$ is obtained from P by a Chvátal cut. Using Farkas' lemma (see Schrijver [28]), we have that Theorem 1 is equivalent to the following geometric result.

Theorem 1′. *For each natural number n there exists an integer g_n such that if P is any polyhedron of dimension n which contains no integral points, then there exists a sequence of polyhedra $P = P_0, P_1, \ldots, P_k = \emptyset$, where $k \leq g_n$ and for each $i = 1, \ldots, k$, P_i is obtained from P_{i-1} by a Chvátal cut.*

In the proof of this geometric result, we will need the following lemma of Schrijver, which is contained in the proof of the main theorem of [27].

Lemma 2. *Let F be a face of a polyhedron P. If $\bar{F}$ is obtained from F by a Chvátal cut, then there exists a polyhedron $\bar{P}$ that can be obtained from P by a Chvátal cut such that $\bar{P} \cap F \subseteq \bar{F}$.*

Proof. Let $P = \{x : A^0 x \leq b^0, A^1 x \leq b^1\}$ where A^0 and b^0 are integral and $F = \{x : A^0 x = b^0, A^1 x \leq b^1\}$ and let $cx \leq \alpha$ be a valid inequality for F such that c is integral and $\bar{F} = F \cap \{x : cx \leq \lfloor \alpha \rfloor\}$. By Farkas' lemma, there exist vectors $y^1 \geq 0$ and y^0 such that

$$\begin{aligned} y^0 A^0 + y^1 A^1 &= c, \\ y^0 b^0 + y^1 b^1 &\leq \alpha. \end{aligned} \tag{7}$$

Defining c' and α' as

$$\begin{aligned} c' &= c - \lfloor y^0 \rfloor A^0 = (y^0 - \lfloor y^0 \rfloor) A^0 + y^1 A^1, \\ \alpha' &= \alpha - \lfloor y^0 \rfloor b^0 \geq (y^0 - \lfloor y^0 \rfloor) b^0 + y^1 b^1 \end{aligned} \tag{8}$$

we have that c' is integral (since $\lfloor y^0 \rfloor A^0$ is integral) and that $c'x \leq \alpha'$ is valid for P (since $y^0 - \lfloor y^0 \rfloor$ is nonnegative). Now letting $\bar{P} = P \cap \{x : c'x \leq \lfloor \alpha' \rfloor\}$ we have

$$\begin{aligned}\bar{P}\cap F &= F\cap\{c'x\le\lfloor\alpha'\rfloor\}\\ &= F\cap\{x: c'x\le\lfloor\alpha'\rfloor, \lfloor y^0\rfloor A^0x=\lfloor y^0\rfloor b^0\}\\ &\subseteq F\cap\{x: cx\le\lfloor\alpha\rfloor\}=\bar{F}. \qquad \square\end{aligned} \tag{9}$$

Proof of Theorem 1′. We proceed by induction on n. The result being clear if $n=0$, let $P\subseteq\mathbb{Q}^m$ be a polyhedron of dimension $n\ge 1$ with $P\cap\mathbb{Z}^m=\emptyset$. We first argue that we may assume P is of full dimension, that is $n=m$. If this is not the case, then P lies in a hyperplane $J=\{x\in\mathbb{Q}^m: cx=\alpha\}$ where c is integral with relatively prime components. If α is nonintegral, then $\emptyset$ can be obtained from P by the Chvátal cut $\{x\in\mathbb{Q}^m: cx\le\lfloor\alpha\rfloor\}$. If α is integral, then J contains integral points, which implies that there exists an affine transformation T which maps J onto $\{x\in\mathbb{Q}^m: x_m=0\}$ and Z^m onto Z^m. (One way to see this is as follows: let w be an integral vector in J and translate J by $-w$ to obtain the linear space $L=J-w$ parallel to J. Now let $b_1,\dots,b_m$ be a basis for the lattice $\mathbb{Z}^m$ such that $b_1,\dots,b_{m-1}$ is a basis for the $(m-1)$-dimensional lattice $L\cap\mathbb{Z}^m$. If we define a linear transformation M by setting $M(b_i)=e_i$ for $i=1,\dots,m$, where e_i is the ith unit-vector, then letting $T(x)=M(x)-w$, we have the required affine transformation.) If we have a sequence of polyhedra $R_0,\dots,R_k$ in $\mathbb{Q}^{m-1}$ where $R_0=\{y\in\mathbb{Q}^{m-1}: (y,0)\in T(P)\}$, $R_k=\emptyset$, and for $i=1,\dots,k$, R_i is obtained from R_{i-1} by a Chvátal cut, then defining P_i to be $\{x\in\mathbb{Q}^m: T(x)=(\bar{y},0)$ for some $\bar{y}\in R_i\}$ for $i=0,\dots,k$, we have $P_0=P$, $P_k=\emptyset$, and for $i=1,\dots,k$, P_i is obtained from P_{i-1} by a Chvátal cut. As the dimension of $\{y\in\mathbb{Q}^{m-1}: (y,0)\in T(P)\}$ is equal to the dimension of P, it suffices to prove the result for $\{y\in\mathbb{Q}^{m-1}: (y,0)\in T(P)\}$. Since we may repeat this procedure, we may assume that P is of full dimension, as claimed.

It follows from a result of Lenstra [22] and Grötschel, Lovász, and Schrijver [15] that, since P contains no integral points, there exists a nonzero integral vector w such that $|wx-wx'|<\gamma_n$ for all $x,x'\in P$, where γ_n is a constant which depends only on n. Let $\beta=\lfloor\max\{wx: x\in P\}\rfloor$ and let $P_1=P\cap\{x\in\mathbb{Q}^m: wx\le\beta\}$. If $P_1=\emptyset$ we are finished, so suppose this is not the case. Let $F=P_1\cap\{x\in\mathbb{Q}^m: wx=\beta\}$. Since $n=m$, the face F is a polyhedron of dimension less than n. We may assume, by induction, that there exists a sequence of polyhedra $F=F_0,F_1,\dots,F_j=\emptyset$ where $j\le g_{n-1}$, and for $i=1,\dots,j$, F_i is obtained from F_{i-1} by a Chvátal cut. By Lemma 2, this implies the existence of a sequence of polyhedra $P_1,P_2,\dots,P_{j+1}$ such that for $i=2,\dots,j+1$, P_i is obtained from P_{i-1} by a Chvátal cut and $P_i\cap\{x\in\mathbb{Q}^m: wx=\beta\}\subseteq F_{i-1}$. So $P_{j+1}\cap\{x\in\mathbb{Q}^m: wx=\beta\}=\emptyset$ and $\{x\in\mathbb{Q}^m: wx\le\beta-1\}$ is a Chvátal cut for P_{j+1}. Let $P_{j+2}=P_{j+1}\cap\{x\in\mathbb{Q}^m: wx\le\beta-1\}$. Since $P\subseteq\{x\in\mathbb{Q}^m: wx>\beta-\gamma_n\}$, repeating this procedure at most γ_n-1 times we obtain the empty set. Thus, letting $g_n=\gamma_n(1+g_{n-1})+1$, the result follows. $\square$

One may wonder why we have only considered the length of a cutting-plane proof of $cx\le\alpha$ from (1) and not its size, that is the size of the linear system (3) plus the size of the nonnegative numbers y_{kj} $(1\le k\le M, 1\le j\le m+k-1)$, which is a more

accurate measure of the complexity of the proof. A partial justification of this is the following result, which is proved using Carathéodory's theorem and is used in the next section (see also Chvátal [7, Theorem 3]).

Proposition 3. *A cutting-plane proof of an inequality $cx \leq \alpha$ from a linear system $Ax \leq b$ implies the existence of one of the same length and with size bounded above by a polynomial function of the length of the proof and the sizes of $cx \leq \alpha$ and $Ax \leq b$.*

Proof. Suppose we have a linear system in n variables

$$a_i x \leq b_i \quad (i = 1, \ldots, m) \tag{10}$$

and a sequence of inequalities

$$a_{m+i} x \leq b_{m+i} \quad (i = 1, \ldots, t) \tag{11}$$

which, together with the nonnegative numbers $y_{m+k,j}$ $(1 \leq k \leq t, 1 \leq j \leq m+k-1)$, is a cutting-plane proof of $cx \leq \alpha$ from (10). By scaling if necessary, we may assume that $a_1, \ldots, a_m, c$ and $b_1, \ldots, b_m, \alpha$ are integral. Let σ denote the maximum of the absolute values of the numbers appearing in (10) and $cx \leq \alpha$. We will show, by induction on t, that there exists a sequence of inequalities

$$a'_{m+i} x \leq b'_{m+i} \quad (i = 1, \ldots, t) \tag{12}$$

and nonnegative numbers $y'_{m+k,j}$ $(1 \leq k \leq t, 1 \leq j \leq m+k-1)$ which together form a cutting-plane proof of $cx \leq \alpha$, where for $i = 1, \ldots, t$ the vector (a'_{m+i}, b'_i) has components which are at most $(n+1)^i \sigma$ in absolute value. The theorem will follow from this, since this implies that the size of (12) is polynomial in t and the sizes of (10) and $cx \leq \alpha$, and since we may assume that the size of the numbers y'_{kj} $(1 \leq k \leq t,$ $1 \leq j \leq m+k-1)$ is polynomial in the size of (12), as for each $k \in \{1, \ldots, t\}$ we may replace $y'_{m+k,j}$ $(1 \leq j \leq m+k-1)$ by any solution of the linear system

$$\begin{aligned} &\sum \{z_i a_i : i = 1, \ldots, m\} + \sum \{z_i a'_i : i = m+1, \ldots, m+k-1\} = a'_{m+k}, \\ &\sum \{z_i b_i : i = 1, \ldots, m\} + \sum \{z_i b'_i : i = m+1, \ldots, m+k-1\} < b'_{m+k} + 1, \\ &\quad z_i \geq 0 \quad (i = 1, \ldots, m+k-1). \end{aligned} \tag{13}$$

(and there exists such a solution with size polynomial in the size of (13)).

The existence of the sequence of inequalities (12) is trivial if $t \leq 1$. Suppose $t \geq 2$ and let $\beta = \sum \{y_{m+1,j} b_j : j = 1, \ldots, m\}$. By Carathéodory's theorem the linear system

$$\begin{aligned} &\sum \{z_{m+1,j} a_j : j = 1, \ldots, m\} = a_{m+1}, \\ &\sum \{z_{m+1,j} b_j : j = 1, \ldots, m\} = \beta, \\ &\quad z_{m+1,j} \geq 0 \quad (j = 1, \ldots, m) \end{aligned} \tag{14}$$

has a solution $\bar{y}_{m+1,j}$ $(1 \leq j \leq m)$ with at most $n+1$ nonzero variables. (The system

clearly has a solution, namely $y_{m+1,j}$ $(1 \leq j \leq m)$.) Let

$$\begin{aligned} a^*_{m+1} &= \sum \{(\bar{y}_{m+1,j} - \lfloor \bar{y}_{m+1,j} \rfloor) a_j : j = 1, \ldots, m\}, \\ b^*_{m+1} &= \lfloor \sum \{(\bar{y}_{m+1,j} - \lfloor \bar{y}_{m+1,j} \rfloor) b_j : j = 1, \ldots, m\} \rfloor, \\ y^*_{m+1,j} &= \bar{y}_{m+1,j} - \lfloor \bar{y}_{m+1,j} \rfloor \quad (j = 1, \ldots, m). \end{aligned} \tag{15}$$

Note that

$$\begin{aligned} a_{m+1} &= a^*_{m+1} + \sum \{\lfloor \bar{y}_{m+1,j} \rfloor a_j : j = 1, \ldots, m\}, \\ \lfloor \beta \rfloor &= b^*_{m+1} + \sum \{\lfloor \bar{y}_{m+1,j} \rfloor b_j : j = 1, \ldots, m\}. \end{aligned} \tag{16}$$

Thus, for $k = 2, \ldots, t$, letting

$$\begin{aligned} \bar{y}_{m+k,j} &= y_{m+k,j} + y_{m+k,m+1} \lfloor \bar{y}_{m+1,j} \rfloor \quad (j = 1, \ldots, m) \\ \bar{y}_{m+k,j} &= y_{m+k,j} \quad (j = m+1, \ldots, m+k-1) \end{aligned} \tag{17}$$

we have

$$\begin{aligned} &\sum \{\bar{y}_{m+k,j} a_j : j = 1, \ldots, m+k-1, j \neq m+1\} + \bar{y}_{m+k,m+1} a^*_{m+1} = a_{m+k}, \\ &\lfloor \sum \{\bar{y}_{m+k,j} b_j : j = 1, \ldots, m+k-1, j \neq m+1\} + \bar{y}_{m+k,m+1} b^*_{m+1} \rfloor \leq b_{m+k}. \end{aligned} \tag{18}$$

So

$$a_{m+i} x \leq b_i \quad (i = 2, \ldots, t) \tag{19}$$

together with the nonnegative numbers $\bar{y}_{m+k,j}$ $(2 \leq k \leq t, 1 \leq j \leq m+k-1)$ is a cutting-plane proof of $cx \leq \alpha$ from the system

$$\begin{aligned} a_i x &\leq b_i \quad (i = 1, \ldots, m), \\ a^*_{m+1} x &\leq b^*_{m+1}. \end{aligned} \tag{20}$$

As the length of this proof is $t-1$, we may assume inductively that there exists a sequence of inequalities

$$a^*_{m+i} x \leq b^*_{m+i} \quad (i = 2, \ldots, t) \tag{21}$$

and nonnegative numbers $y^*_{m+k,j}$ $(2 \leq k \leq t, 1 \leq j \leq m+k-1)$ which together form a cutting-plane proof of $cx \leq \alpha$ from (20), where for $i = 2, \ldots, t$ the vector (a^*_{m+i}, b^*_{m+i}) has components which are at most $(n+1)^{i-1}\sigma^*$ in absolute value, letting σ^* denote the maximum of σ and the absolute values of the components of (a^*_{m+1}, b^*_{m+1}). Using this, we have that

$$a^*_{m+i} x \leq b^*_{m+i} \quad (i = 1, \ldots, t) \tag{22}$$

together with the nonnegative numbers $y^*_{m+k,j}$ $(1 \leq k \leq t, 1 \leq j \leq m+k-1)$ is the required cutting-plane proof of $cx \leq \alpha$ from (10). Indeed, from (16) we have that

a^*_{m+1} is integral and hence that (22) is a cutting-plane proof of $cx \leq \alpha$ from (10). Furthermore, since at most $n+1$ of the nonnegative numbers $\bar{y}_{m+1,j}$ $(1 \leq j \leq m)$ are nonzero, from (15) we have that the absolute value of each component of (a^*_{m+1}, b^*_{m+1}) is at most $(n+1)\sigma$. Thus for each $i = 1, \ldots, t$ the components of (a^*_{m+1}, b^*_{m+1}) are at most $(n+1)^i\sigma$ in absolute value. □

Remarks. (1) Cutting planes may be viewed geometrically as a method of obtaining a linear description of the convex hull, P_I, of integer points contained in a given polyhedron $P \subseteq \mathbb{Q}^n$. Letting P' denote the set of vectors which satisfy every Chvátal cut for P, we have that $P_I \subseteq P'$. Schrijver [27] proved that P' is a polyhedron, which can be seen by noting that, as in the proof of Proposition 3, we may restrict our attention to cutting planes that can be derived from at most n valid inequalities for P, each with a nonnegative multiplier less that 1. The results of Chvátal [5] and Schrijver [27] mentioned in Section 1 give that $P^{(k)} = P_I$ for some natural number k, where $P^{(0)} = P$ and $P^{(i)} = P^{(i-1)'}$ for all $i \geq 1$. (In fact, this is the way in which the results are presented in Schrijver [27].) The least number k such that $P^{(k)} = P_I$ is the *Chvátal rank* of P. Using Carathéodory's theorem, Chvátal [7, Theorem 3] proved a result which gives an upper bound on the length of a shortest cutting-plane proof of an inequality from a linear system $Ax \leq b$ in terms of the number of variables and the Chvátal rank of $\{x : Ax \leq b\}$.

The example of Bondy given above shows that polyhedra in 2-space can have arbitrarily high Chvátal rank. However, if $P \subseteq \mathbb{Q}^n$ and $P \cap \mathbb{Z}^n = \emptyset$, then Theorem 1′ implies that $P^{(t_n)} = \emptyset$, where t_n is a constant which depends only on n. This result is used in Cook, Gerards, Schrijver, and Tardos [11] to show that the Chvátal rank of a polyhedron $\{x : Ax \leq b\}$ can be bounded above by a function of the matrix A, independent of the vector b.

(2) Not surprisingly, the number g_n in Theorem 1′ is necessarily exponential in n. What follows from the proof of Theorem 1′ and Proposition 3, is that $2^n/n - 1 \leq \gamma^*_n \leq n^{3n}$, where γ^*_n is the least possible value of γ_n. To see the lower bound, consider the linear system in the variables $x_1, \ldots, x_n$

$$\sum \{x_i : i \in J\} - \sum \{x_i : i \in \{1, \ldots, n\} \setminus J\} \leq |J| - 1 \quad \forall J \subseteq \{1, \ldots, n\} \tag{23}$$

where each inequality cuts off exactly one corner of the unit hypercube. This system has no integral solution, but if an inequality for any set J is removed, then the 0–1 vector $x_i = 1$ for each $i \in J$ and $x_i = 0$ for each $i \in \{1, \ldots, n\} \setminus J$ satisfies the remaining $2^n - 1$ inequalities in the system. Thus any cutting-plane proof of $0x \leq -1$ from (23) must make use of each inequality (that is, each inequality in (23) must be given a positive multiplier in at least one of the derivations in the proof). Now, as in the proof of Proposition 3, if there exists a cutting-plane proof of length of $0x \leq -1$ from (23), then there also exists one of length at most t which uses at most n positive multiplies at each step (except possibly the last, where $n+1$ positive multiplies may be needed). Since each of the 2^n inequalities in (23) must be used in the proof (and since each derived inequality must also be used), t must be at least $2^n/n$. Hence the

shortest sequence of polyhedra as described in Theorem 1′ must have length at least $2^n/n-1$. (Note that this example cannot be improved by replacing (23) by a system which has more that 2^n inequalities, since Scarf [26] (see also Bell [2], Hoffman [19], and Todd [29]) has shown that any system of linear inequalities in n variables having no integral solution contains a subsystem of at most 2^n inequalities which also has no integral solution.)

To prove the upper bound, we need information on the parameter γ_n given in the proof of Theorem 1′, that is, the $\mathbb{Z}^n$-width of a polyhedron in $\mathbb{Q}^n$ which contains no integral vectors. Various upper bounds on γ_n which can be obtained algorithmicly are given in Lenstra [12], Grötschel, Lovász, and Schrijver [15] and Babai [1] (see also Kannan [20]). Each of these bounds is exponential in n. Hastad [17] has recently shown, however, that a result of Lenstra and Schnorr [23] implies that one may let $\gamma_n = n^{5/2}$ (a bound which is not known to be obtainable by a polynomial-time algorithm).

Using this and following the proof of Theorem 1′, it is a simple estimation to obtain n^{3n} as an upper bound on g_n^*. (For other results on lattice-width see Kannan and Lovász [21].)

In the case $n=2$, the bounds can be improved as follows. It can be checked that obtaining the empty set from the polyhedron P given by the convex hull of the points $\{(\frac{1}{2},\frac{5}{4}),(\frac{1}{2},-\frac{1}{4}),(-\frac{1}{2},\frac{1}{2}),(\frac{3}{2},\frac{1}{2})\}$ requires four cutting planes. (First check that P' is given by the convex hull of $\{(\frac{1}{2},0),(\frac{1}{2},1),(0,\frac{1}{3}),(0,\frac{2}{3}),(1,\frac{1}{3}),(1,\frac{2}{3})\}$ and then that P' requires three cutting planes.) Furthermore, Helfrich [18] has shown that we may take $\gamma_2=2$, which implies that the empty set may be obtained from any polyhedron of dimension 2 in at most 5 cuts. So $4\leq g_2^*\leq 5$. □

3. Cutting-plane proofs of unsatisfiability

Formulae of the propositional calculus are built up from variables using negation, conjunction and disjunction. (For an introduction to the propositional calculus see Chang and Lee [4].) A literal is an unnegated or negated variable. A clause $C=\{l_1,\dots,l_k\}$ is a set of literals interpreted as their disjunction (an empty clause is defined to be false). A formula in conjunctive normal form (or CNF-formula) $\varphi=\{C_1,\dots,C_r\}$ is a set of clauses interpreted as their conjunction. A formula is unsatisfiable if it is false under all truth assignments. The size of a formula φ is the number of literals in φ.

Let C_1, C_2 be clauses such that C_1 contains x, C_2 contains $\bar{x}$ and there is no other literal l in C_1 such that $\bar{l}$ is in C_2. Then the clause $C=C_1\cup C_2-\{x,\bar{x}\}$ is the *resolvent* of C_1 and C_2.

A *resolution derivation* from clauses $C_1,\dots,C_r$ is a sequence of clauses $C_1^*,\dots,C_s^*$ such that C_i^* $(1\leq i\leq s)$ is the resolvent of two clauses from $C_1,\dots,C_r, C_1^*,\dots,C_{i-1}^*$. The *length* of the derivation is s. A *resolution proof of a clause* C from clauses $C_1,\dots,C_r$ is a resolution derivation with $C_s^*=C$. A *resolution proof of the unsatis-*

fiability of a CNF-formula $\varphi\{C_1, \ldots, C_r\}$ is a resolution proof of the empty clause from $C_1, \ldots, C_r$. A CNF-formula is unsatisfiable if and only if its unsatisfiability has a resolution proof (Robinson [25]).

An *extended resolution* (e.r.) *derivation* from clauses $C_1, \ldots, C_r$ is defined recursively:

(1)If $C_1^*, \ldots, C_i^*$ is an e.r. derivation and C_{i+1}^* is a resolvent of two clauses from $C_1, \ldots, C_r, C_1^*, \ldots, C_i^*$, then $C_1^*, \ldots, C_{i+1}^*$ is an e.r. derivation.

(2) If $C_1^*, \ldots, C_i^*$ is an e.r. derivation, x and y are variables occuring in $C_1, \ldots, C_r, C_1^*, \ldots, C_i^*$ and z is a new variable then

(a) $C_1^*, \ldots, C_i^*, \{z, x\}, \{\bar{z}, \bar{x}\}$ is an e.r. derivation;

(b) $C_1^*, \ldots, C_i^*, \{z, \bar{x}\}, \{z, \bar{y}\}, \{\bar{z}, x, y\}$ is an e.r. derivation.

Thus it is possible to introduce new variables $z \equiv \bar{x}$, $z \equiv x \vee y$ (the new clauses are the CNF for these functions). *Length, e.r. proof of a clause* and *e.r. proof of unsatisfiability* are defined as for resolution.

Our purpose here is to compare the power of resolution and extended resolution with that of cutting planes. We begin by describing cutting planes as a system for proving the unsatisfiability of CNF-formulae.

For a literal l let $E(l) := x$ if $l = x$ and $E(l) := 1 - x$ if $l = \bar{x}$. For a clause $C = \{l_1, \ldots, l_k\}$ let $E(C) = \sum_{i=1}^{k} E(l_i)$. ($E(\emptyset) := 0$.) For a CNF-formula $\varphi = \{C_1, \ldots, C_r\}$ containing variables $x_1, \ldots, x_m$ let $\mathscr{E}(\varphi)$ be the following system of $2m + r$ inequalities:

$$E(C_i) \geq 1 \quad (1 \leq i \leq r), \qquad 0 \leq x_j \leq 1 \quad (1 \leq j \leq m). \tag{24}$$

A *cutting-plane proof of the unsatisfiability of* φ is a cutting-plane proof of $0 \geq 1$ from $\mathscr{E}(\varphi)$.

It is easy to see that φ is unsatisfiable if and only if $\mathscr{E}(\varphi)$ has no integral solution, hence φ's unsatisfiability has a cutting-plane proof.

Resolution can be simulated by cutting-planes using the following lemma:

Lemma 4. *If clause C is the resolvent of clauses C_1, C_2, then $E(C) \geq 1$ has a cutting-plane proof of length 1 from*

$$E(C_1) \geq 1, \quad E(C_2) \geq 1, \quad 0 \leq x_i \leq 1, \quad 1 \leq i \leq m.$$

Proof. Let $C_1 = \{x_1, l_1, \ldots, l_k, l_{k+1}, \ldots, l_{k_1}\}$, $C_2 = \{\bar{x}_1, l_1, \ldots, l_k, l'_{k+1}, \ldots, l'_{k_2}\}$ (thus $l_1, \ldots, l_k$ are the common literals in C_1 and C_2). Then adding

$$E(C_1) = x_1 + \sum_{i=1}^{k} E(l_i) + \sum_{i=k+1}^{k_1} E(l_i) \geq 1,$$

$$E(C_2) = (1 - x_1) + \sum_{i=1}^{k} E(l_i) + \sum_{i=k+1}^{k_2} E(l'_i) \geq 1,$$

$$E(l_i) \geq 0 \quad (k+1 \leq i \leq k_1), \qquad E(l'_i) \geq 0 \quad (k+1 \leq i \leq K_2),$$

we get

$$2\left(\sum_{i=1}^{k} E(l_i) + \sum_{i=k+1}^{k_1} E(l_i) + \sum_{i=k+1}^{k_2} E(l_i')\right) \geq 1$$

and by rounding

$$E(C) = \sum_{i=1}^{k} E(l_i) + \sum_{i=k+1}^{k_1} E(l_i) + \sum_{i=k+1}^{k_2} E(l_i') \geq 1. \qquad \square$$

Proposition 5. *If the unsatisfiability of a CNF-formula φ has a resolution proof of length s, then it has a cutting-plane proof of length s containing only inequalities with 0 and ± 1 coefficients.*

Proof. Obvious from the above lemma. □

So cutting planes are at least as powerful as resolution. To proceed further, consider the following 'pigeonhole formulae' that were introduced by Cook and Reckhow [10] to illustrate the power of extension.

For variables x_{ij} $(1 \leq i \leq n,\ 1 \leq j \leq n-1)$ define

$$\varphi_n \leftrightarrow \bigwedge_i \left(\bigvee_j x_{ij}\right) \wedge \bigwedge_{i_1 \neq i_2} \bigwedge_j (\bar{x}_{i_1, j} \vee \bar{x}_{i_2, j}). \tag{25}$$

These formulae are unsatisfiable, as a satisfying truth assignment would give a bijection between $\{1, \ldots, n\}$ and $\{1, \ldots, n-1\}$. Of particular interest here is the following result of Haken [16].

Theorem 6. *There is no polynomial upper bound on the length of a shortest resolution proof of the unsatisfiability of the formulae φ_n.* □

This theorem together with the following proposition implies that cutting planes are more powerful than resolution.

Proposition 7. *The unsatisfiability of φ_n has a cutting-plane proof of length n^3.*

Proof. The corresponding system of inequalities is

$$\sum_{j=1}^{n-1} x_{ij} \geq 1 \quad (i = 1, \ldots, n), \tag{26}$$

$$x_{i_1 j} + x_{i_2 j} \leq 1 \quad (1 \leq i_1 < i_2 \leq n,\ j = 1, \ldots, n-1), \tag{27}$$

$$0 \leq x_{ij} \leq 1 \quad (i = 1, \ldots, n,\ j = 1, \ldots, n-1).$$

It is sufficient to deduce the inequalities

$$\sum_{i=1}^{n} x_{ij} \leq 1 \quad (j = 1, \ldots, n-1). \tag{28}$$

as then summing (26) and (28) a contradiction is obtained. To get (28) we show that for every $j=1,\ldots,n-1$, $r=1,\ldots,n-1$ and $i=1,\ldots,n-r$

$$\sum_{k=i}^{i+r} x_{kj} \leq 1. \tag{29}$$

This follows by induction on r, the case $r=1$ is contained in (26). For the induction step,

$$\sum_{k=i}^{i+r} x_{kj} \leq 1, \qquad \sum_{k=i+1}^{i+r+1} x_{kj} \leq 1, \qquad x_{ij} + x_{i+r+1,j} \leq 1$$

imply $2\sum_{k=i}^{i+r+1} x_{kj} \leq 3$ and by rounding $\sum_{k=i}^{i+r+1} x_{kj} \leq 1$. As one cut is needed to generate a new inequality, the bound follows. □

Now we turn to the relationship between extended resolution and cutting planes.

Theorem 8. *There exists a polynomial $p(n, m)$ such that for every unsatisfiable CNF-formula φ of size m, if the unsatisfiability of φ has a cutting-plane proof of length n, then it has an extended resolution proof of length at most $p(n, m)$.*

Proof. The proof is based on a general result of Cook [9] on the power of extended resolution. Here we assume the notions and results of [9] without giving the detailed formulation. We also refer to the thesis of Dowd [12], where Cook's results are proven in detail and generalized, and to the book of Goodstein [14] for rigorous formal proofs in a restricted arithmetic system called primitive recursive arithmetic (which was further restricted by Cook to obtain his system PV).

First we note that the length of a cutting-plane proof in the theorem refers to number of inequalities, while in the framework of Cook's paper the length of a proof means the number of digits of the whole (encoded) proof, which is polynomially related to the sum of the sizes of the inequalities, where the size of the coefficients is counted as well. However, Proposition 3 of the previous section implies that from our point of view the two definitions are equivalent. (At the beginning, every coefficient on the left-hand sides is ± 1, and every coefficient on the right-hand sides is at most m.)

The main result of [9] (Theorem 5.5, see also Theorem IV.4.1 of [12]) implies that it is sufficient to show, that the cutting-plane-proof system is *p-verifiable* (see Definition 5.4 of [9]). Informally, this means that the statement

> "If x is a cutting-plane proof of the unsatisfiability of a CNF-formula y, then y is indeed unsatisfiable",

expressing the *correctness* of the proof system, can be formulated and proven in the formal system PV.

A technical detail here is that [9] defines proof systems (including extended resolution) for proving that propositional formulae are tautologies. However, cutting planes can also be considered as a proof system for tautologies (proving that the negation of the formula is unsatisfiable), and it is also easy to see that the two versions of extended resolution are equivalent.

Below we give an informal description of the proof of the p-verifiability of cutting planes. References are given to the results and proofs of [9], [12] and [14], that can be used to give a more formal proof (which would contain no technical novelties).

The p-verifiability of cutting planes is proven in the following stages.

Stage 1. Arithmetic on integers and rationals (as pairs of integers) is defined. This is possible, as Theorem 2.12 of [9] states that every polynomial-time computable function is definable in PV. (See also Theorem II.4.1 of [12], where a proof is given.)

Stage 2. Propositions involving linear inequalities and rounding are proven. Theorem 3.11 of [9] states that every proof of a universal sentence from universal sentences in the usual predicate calculus can be translated into a system PV1. Theorem 3.10 of [9] states that PV1 proofs can be translated into PV proofs. (This is Theorem II.5.1 of [12], where the result is proven.) Detailed formal proofs which can be translated into PV1 are given for such identities in section 2.96 of [14].

Stage 3. The p-verifiability of cutting planes is proved by formalizing the proofs of the propositions referred to above. Section 4 of [9] and section II.6 of [12] discuss the definition and properties of a Gödel numbering. For example, the function $f(x, i) :=$ "the Gödel number of the i-th inequality in the cutting-plane proof encoded by x, or 0 if this is not defined" can be defined using the function $ELEM(x, i)$ of [12, p. 31]. The formalized versions of statements such as "If the integer y satisfies the first i inequalities in the cutting-plane proof x, then it also satisfies the $i+1$-st one" imply the p-verifiability of the cutting-plane proof system, in the same way that the proof of the soundness of extended resolution is used to prove the p-verifiability of extended resolution (see Lemma 5.8 of [9] and Section IV.2 of [12]). □

This implies that extended resolution is at least as powerful as cutting plane proofs of unsatisfiability. We have not been able to show that extended resolution is the more powerful of the two systems, a proof of which would involve showing that the cutting-plane proof system is nonpolynomial.

Remark. The geometric analogue of extension by $Z \equiv x \vee y$ is a 'lifting' of the polytope determined by the actual clauses to a higher-demensional one by adding a new variable z and inequalities $0 \leq z \leq 1$, $x \leq z$, $y \leq z \leq x+y$. It is not clear how such a lifting operation influences the number of cuts required to reduce a polyhedron to the empty set. □

Acknowledgement

The authors would like to thank Professor Ravi Kannan for a number of valuable discussions on the lattice-width of polyhedra.

References

[1] L. Babai, On Lovász' lattice reduction and the nearest lattice point, Combinatorica, to appear.

[2] D.E. Bell, A theorem concerning the integer lattice, Stud. Appl. Math. 56 (1977) 187–188.

[3] S.C. Boyd and W.R. Pulleyblank, Facet generating techniques, in preparation.

[4] C.L. Chang and R.C.T. Lee, Symbolic Logic and Mechanical Theorem Proving (Academic Press, New York, 1973).

[5] V. Chvátal, Edmonds polytopes and a hierarchy of combinatorial problems, Discrete Math. 4 (1973) 305–337.

[6] V. Chvátal, Edmonds polytopes and weakly hamiltonian graphs, Math. Programming 5 (1973) 29–40.

[7] V. Chvátal, Cutting-plane proofs and the stability number of a graph, Report No. 84326-OR, Inst. für Ökon. u. Operations Research, Uni. Bonn, W. Germany, 1984.

[8] V. Chvátal, Cutting planes in combinatorics, Report No. 84325-OR, Inst. für Ökon. u. Operations Research, Uni. Bonn, W. Germany, 1984.

[9] S.A. Cook, Feasibly constructive proofs and the prop ositional calculus, Proc. 7th ACM Symp. on the Theory of Comp uting (1975) 83–97.

[10] S.A Cook and R.A. Reckhow, The relative efficiency of propositional proof systems, J. Symbolic Logic 44 (1977) 36–50.

[11] W. Cook, A.M.H. Gerards, A. Schrijver and É. Tardos, Sensitivity theorems in integer linear programming, Math. Programming, to appear.

[12] M. Dowd, Propositional representation of arithmetic proofs, Ph. D. Thesis, Univ. of Toronto, 1979.

[13] R.E. Gomory, An algorithm for integer solutions to linear programs, in: R.L. Graves and P. Wolfe, eds., Recent Advances in Mathematical Programming (McGraw-Hill, New York, 1963) 269–302.

[14] R.L. Goodstein, Recursive Number Theory (North-Holland, Amsterdam, 1957).

[15] M. Grötschel, L. Lovász and A. Schrijver, The Ellipsoid Method and Combinatorial Optimization (Springer, Berlin, to appear).

[16] A. Haken, The intractability of resolution, Theor. Comput. Sci. 39 (1985) 297–308.

[17] J. Hastad, communicated by R. Kannan.

[18] B. Helfrich, Eine Beziehung zwischen konvexen Mengen $P \subset \mathbb{R}^2$ und den Gitterbasen von $\mathbb{Z}^2$, Manuscript, Frankfurt, W. Germany, 1985.

[19] A.J. Hoffman, Binding constraints and Helly numbers, Research Report, IBM T.J. Watson Research Center, 1977.

[20] R. Kannan, Imkproved algorithms for integer programming and related lattice problems, 15th ACM Symkp. on the Theory of Computing (1983) 193–206.

[21] R. Kannan and L. Lovász, to appear.

[22] H.W. Lenstra, Jr., Integer programming with a fixed number of variables, Math. Oper. Res. 8 (1983) 538–548.

[23] H.W. Lenstra, Jr. and C.P. Schnorr, On the successive minima of a pair of polar lattices, to appear.

[24] L. Lovász, An algorithmic theory of numbers, graphs and convexity, Report No. 85368-OR, Inst. für Ökon. u. Operations Research, Uni. Bonn, W. Germany, 1985.

[25] J.A. Robinson, A machine-oriented logic based on the resolution principle, JACM (1965) 23–41.

[26] H.E. Scarf, An observation on the structure of production sets with indivisibilities, Proc. Nat. Acad. Sci. (USA) 74, 3637–3641.

[27] A. Schrijver, On cutting planes, Ann. Discrete Math. 9 (1980) 291–296.

[28] A. Schrijver, Theory of Linear and Integer Programming (Wiley, Chichester, 1986).

[29] M.J. Todd, The number of necessary constraints in an integer program: a new proof of Scarf's theorem, Report No. 355, School of Oper. Res. and Ind. Eng., Cornell Univ., Ithaca, NY, USA, 1977.

[30] G.S. Tseitin, On the complexity of derivations in the propositional calculus, in: A.O. Slisenko, ed., Structures in Constructive Mathematics and Mathematical Logic, Part II (translated from Russian, 1968) 115–125.